I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to:

ASSISTANT COMMISSIONER OF PATENTS
WASHINGTON, DC 20231

bearing Label Number EE 651 410 479 US and mailed December 6, 1999.

MIRIAM DAVIS
Print Name

Miriam Davis
Signature

PATENTS

Inventors: Richard Alan Dayan
Eric Richard Kern

METHOD AND SYSTEM FOR SECURING A PERSONAL COMPUTER BUS

Cross Reference to Related Patents

The present invention is related to U.S. Patent 4,460,957 entitled "Self Pacing Serial Keyboard Interface for a Data Processing System" which is assigned to the assignee of the present invention. The teachings of this patent, which is sometimes referred to as the Keyboard Patent, are hereby specifically incorporated into this document by reference.

Sub A1

The present invention is also related to two patent applications related to the selective locking of a keyboard. These patent applications, which are sometimes referred to as the ROM Scan Applications, are Serial No. 09/052,733 entitled "Personal Computer ROM Scan During Startup Protection" filed March 31, 1998 by

Sub a1

~~Robert Duane Johnson et al. and "Method and System for Improved Security During ROM Scan", Serial No. 09/431,728 filed on November 1, 1999, by Richard Alan Dayan et al. The ROM Scan Applications are assigned to the assignee of the present invention, with the disclosures of these patents specifically incorporated herein by reference.~~

Background of the Invention

Field of the Invention

The present invention is an improved system and method for providing security in a personal computer. More particularly, the present invention relates to securing an external bus (particularly the Universal Serial Bus, sometimes referred to as the USB Interface) and coupling the locked state of that bus with the locked state of the keyboard. This accomplishes security of the external bus consistent with the security of the keyboard.

Background Art

Personal computers in general, and the IBM personal computers in particular, have obtained wide spread use for a variety of data processing applications, providing computing power to many segments of society for handling information in the form of digital data. These personal computers may be defined as desktop, floor-standing or a portable unit and typically include a system unit with a single system processor with volatile and nonvolatile memory, a display, one or more input devices such as a keyboard or a mouse connected to dedicated data ports in the system unit and one or more storage devices such as a floppy disk drive, a fixed disk drive or a CD ROM drive, and optionally, a printer or other output device. The components of a personal computer are assembled into an enclosure which includes a variety of data ports or external connectors to couple input and output devices to the single system processor.

Such personal computers not only include the dedicated port(s) for connecting the keyboard or mouse, but a variety of general purpose buses have been established to interface a wide variety of peripheral devices through well-defined (in some cases, industry-standard or quasi-industry standard) interfaces. One such type of interface is the Universal Serial Bus interface (sometimes referred to as the USB interface), the parameters of which are set forth in a generally available document entitled “Universal Serial Bus Specification” Release 1.1 dated September 23, 1998 from USB.ORG which was prepared by representatives of four companies; Compaq, Intel, Microsoft and NEC. Buses which comply with this standard are referred to as the USB interface and have been included on several recent versions of personal computers from various different manufactures for attaching devices for plug-and-play of personal computers with such computer peripherals as telephones, modems, CD-ROM drives, joysticks, tape and floppy drives, scanner and printers. Additionally, the USB Interface allows an alternate connection for input devices such as keyboards and mice, providing an alternate to the dedicated keyboard and mouse ports which many manufacturers provide.

The ROM Scan Patents disclose that it is sometimes desirable to prevent a user input at an input device such as a keyboard or a mouse, a feature which locks out the keyboard from making effective inputs during sensitive periods such as the initialization of the personal computer during its power-on-self test, POST, and ROM scan. The ROM Scan Patents also teach that the memory of the computer system may be vulnerable to user inputs during these times and that user inputs should be controlled. One such way to control the input is to lock out the keyboard for at least part of the time during which ROM scan is occurring, as taught by the ROM Scan Patents.

In addition, there are other security features which advantageously control the keyboard. When a user leaves his workstation, he can invoke a security feature which locks out the keyboard until a key is used to unlock the system. Some systems also provide security by locking the keyboard during certain time periods and other require the use of a supervisory key to unlock the keyboard for use. Locking of a keyboard may be selectively controlled (by either a physical key or by password or other security control) and is well known in the trade as a desirable feature of current models of personal computers.

However, no locks for the USB port of the personal computer are specified in the document referred to above -- the Universal Serial Bus is generally available whenever the personal computer is powered up. Thus, a keyboard attached through the dedicated keyboard port may be secured against entries, but a similar keyboard accomplishing the same function is not secured at all when attached through the USB port.

Summary of the Invention

The present invention overcomes the disadvantages and limitations of the prior art devices while providing security for the system against devices hooked into it through an external bus such as the USB interface.

The present invention has the advantage that a keyboard lock applied to the keyboard port in a computer system has the effect of locking out an input device attached to the USB Interface.

By synchronizing the locking and unlocking of a keyboard attached to the dedicated keyboard port of a computer system with a USB interface, the system is secure against input devices, whether the input the device is attached to the dedicated port or attached to a USB interface.

The present invention has the advantage that it is a simple, yet effective, way of providing security for the sensitive portions of computer storage during times when they are vulnerable to attack because the operating system is writing to those portions of memory, e.g., during the power-on-self-test. The present invention overcomes the disadvantage in the prior art that the computer could be locked against keyboard input through the keyboard port while remaining open to a keyboard entry through the USB interface where an input device such as a keyboard is one of the devices intended to be connected.

Other objects and advantages of the present invention will be apparent to those skilled in the relevant art in view of the following description of the preferred embodiment, taken together with the accompanying drawings and the appended claims.

Brief Description of the Drawings

Having thus described some of the objects and advantages of the present invention, other objects and advantages of this invention will be apparent through the discussion of the drawings of present invention of an improved computer security system and method in which:

Fig.1 is a pictorial view of a computer system environment useful for understanding the present invention;

Fig. 2 is a block diagram of the computer system of Fig. 1;

Fig. 3 is a block diagram of the Computer System with the Present invention included;

Fig. 4 is a logic diagram for a keyboard sensing unit as shown in Fig. 3.

Fig. 5 is a logic diagram for a Security unit as shown in Fig. 3.

Detailed Description of the Preferred Embodiment

In the following description of the preferred embodiment, the best implementation of practicing the invention presently known to the inventors will be described with some particularity. However, this description is intended as a broad, general teaching of the concepts of the present invention in a specific embodiment but is not intended to be limiting the present invention to that as shown in this embodiment, especially since those skilled in the relevant art will recognize many variations and changes to the specific structure and operation shown and described with respect to these figures. Some of those skilled in the relevant art will also recognize that some of the benefits of the present invention can be obtained by using only some of the features described in connection with the present invention without the corresponding use of other features.

Fig. 1 is a pictorial view of a computer system 10 useful in understanding the present invention. The computer system 10 includes a system unit 12 with two input devices, a keyboard 14 and a mouse 16, coupled to it. The couplings are not shown, but the system unit of many personal computers of recent vintage include dedicated ports for plugging in the keyboard and the mouse because such input devices are ubiquitous. Also shown as a part of the computer system 10 is a display 17, an optional printer 18 and a USB peripheral device 20. Many system units of current model personal computers include interfaces (or plugs) brought out to the outside of the case for specific devices (such as the display 17) and also a variety of general purpose ports into which peripheral devices can be attached, including at least one Universal Serial Bus (USB) interfaces (many personal computers from IBM currently provide two USB ports for attaching peripherals operating using the USB standards references above). The USB peripheral device 20 is plugged into one USB port of the system unit 12 which connects the USB peripheral to a system bus inside the system unit 12.

As described elsewhere in this document in greater detail, the USB interface was designed to accommodate an input or output device selected from a wide variety of potential input/output devices, such as a CD-ROM drive or a keyboard.

The ROM Scan Patents describe the risks associated with the use of a keyboard during initial start up of a personal computer, when the computer goes through power-on-self-test (POST) and performs a ROM scan looking for ROM adapters. The ROM Scan Patents describe the risks as potential data security risks and propose that the keyboard be locked out during that time (unless a user input is required by the ROM adapter). It is proposed in the ROM Scan Patents that the dedicated interface to the keyboard and the mouse be selectively locked out from accepting user inputs during the period of time that the ROM scan is occurring in the computer. The present invention extends the protection (e.g., during the ROM scan activity) against keyboard input from a user to protect the computer system against user input transmitted through a general purpose interface such as the USB port by an input device connected to the USB port. In this way, the computer system is secured against user input during crucial time periods from either an input device connected either through a dedicated port for such an input device or through a general purpose port such as the USB interface. The concepts of the present invention relating to coupling the locking of the keyboard to a locking out of the general purpose port apply as well to times during the operation of the computer system other than the computer start up (e.g., POST and ROM scan) activity when the computer system may be locked against keyboard entries, such as to protect an unattended computer system.

Sub A2

Figure 2 is a schematic diagram of a portion of the personal computer 10. The keyboard 14 is coupled through a keyboard/mouse controller 22 via a Low Pin Count (LPC) or ISA bus 24 to the I/O Controller Hub (ICH) 28 via a Hub Link Bus (HLB) to a Memory Controller Hub (MCH) 27 via a Front Side Bus (FSB) to the central processor 26 of the personal computer 10.

Access by the central processor 10 is via the processors I/O address space

Sub a3

at I/O address space addresses 60 hexadecimal and 64 hexadecimal. The mouse 16 is also coupled to the keyboard/mouse controller 22. Both the keyboard 14 and mouse 16 ports are referred to as the PS/2 Keyboard and PS/2 Mouse ports, respectively in the PC industry. As known in the state of the art, any device that emulates either a keyboard or mouse can attach to the respective port.
In many personal computers, the keyboard 14 and mouse 16 ports are dedicated to their respective devices and are only configured to allow the attachment of such a device.

Figure 3 is a schematic diagram illustrating the locking system of the present invention. The Keyboard/mouse controller 22, which is resident in the Super I/O module 29 and used to connect the keyboard 14 to the microprocessor 26, is connected to a security unit 82 which is a new connection for this invention. Alternative connections are possible to someone familiar with the state of the art.

For example, the security unit 82 could be connected to the LPC bus 24 and monitor the transmissions for commands targeting the keyboard 14 or its controller 22.

The USB host controller 30 is connected to the USB ports 88 via an interposing switch 80. The switch 80 receives instructions from the security unit 82 to instruct the switch 80 to lock or unlock the bus via a control signal 89. When

Sub a2

locked, the switch prevents data from reaching the USB host controller 30 and the microprocessor 24, however, the USB Keyboard sensing unit 84 can still monitor the transmissions from devices attached to the USB ports 88 to monitor for entry of the password in order to unlock the bus 88. As USB keyboard keystrokes are detected, the keyboard sensing unit unpacks the USB usage codes and converts them to the well known PS/2 keyboard scan codes via bus 90 to the security unit 90 for correct password entry verification. When unlocked, the switch allows all USB transmissions from devices attached to the USB ports 88 to the USB host controller 30 and the microprocessor 24. In this way, when the switch 80 is in the locked state and keyboard inputs are not being processed from the USB ports 88 by the microprocessor 26, there is still something in the personal computer (the security unit 82) listening for a correct password to unlock the system and allow direct communication from either the keyboard 14 and/or a USB keyboard attached to one of the USB ports 88.

Figure 4 shows the logic in use in the USB Keyboard Sensing Unit 84 of this invention. The Sensing unit 84 constantly monitors 60 the USB bus 88 for the presence of data and commands.

If data is found, it is checked to see if it is a Control Request 62. If not a control request, the data is checked to see if a USB device is sending data to the controller 70. If it is not a data packet, the sensing unit 84 returns to monitor the

Sub a2

USB bus 60. If a USB data packet is present 70, the sensing unit 84 checks to see if it is from a keyboard device identified 72 in step 68. If not a keyboard data packet, the sensing unit 84 returns to monitor the USB bus 60. If it is keyboard data packet 72, the sensing unit detects the usage code from the data packet 74 and converts the usage code to the industry standard scan code used by the PS/2 Keyboard device 76. The sensing unit 84 then transmits the scan code to the Security Unit 82 for processing and returns to step 60 to monitor the USB bus 88 for more data packets.

Returning to step 62, if the data is a control request, the sensing unit tests to see if it is a USB Keyboard Descriptor 64. If not, the sensing unit returns to its monitoring state in step 60. If the data is a keyboard descriptor 64, the sensing unit looks for an ID command 66. When found, the USB ID is stored so that the USB device is recognized as a USB keyboard. Then processing returns to step 60 where the monitoring process resumes.

Figure 5 illustrates a logic design for the security unit 82 to allow it to recognize a correct password to unlock the keyboard attached to the system when the personal computer (and its processor 26) is otherwise locked against user inputs. The security unit 82 receives, at block 100, a single unit of data, such as would emanate from a single key stroke on a PS/2 personal computer keyboard or a USB keyboard attached at USB interface 88, indicating either a single character

Sub a2

or a command from the processor 26 to the keyboard and checked to see if this data is a Load Password Command from the processor. If it is a Load Password Command, the security unit 82 intercepts and stores the next set of characters as the password until a terminator (00h) is encountered 102. Processing continues at step 100 again.

Returning to step 100, if the data is not a Load Password Command, the security unit 82 checks to see if the data is an Enable Password Command 104 from the processor 26. If not, the security returns to step 100 to monitor the USB bus 88 and PS/2 I/O ports 60h and 64h 86. If the data is an Enable Password command, the security unit 82 checks to see if a valid password is already loaded 106. If not, the security unit returns to step 100 to continue monitoring. If a valid password is already loaded, the security unit 82 locks the switch 80 in step 108. Following locking the keyboard, the security unit 82 goes into a monitoring state to check for the entry of a Valid password 110. The password may be entered on either the PS/2 Keyboard 14 or a USB keyboard attached at the USB interface 88. The system remains locked with respect to keyboard entry until the password is correctly entered. In step 112, the security unit 82 checks to see if the password was entered. If not entered correctly, the security unit 82 go to step 110 to monitor for entry of a password once again. If entered correctly, the switch 80 is unlocked 114 and the security unit 82 start the process over again at step 100.

Of course, many modifications of the present invention will be apparent to those skilled in the relevant art in view of the foregoing description of the preferred embodiment, taken together with the accompanying drawings. The system for locking and unlocking the interface port to the keyboard port can be changed to fit the system requirements and designer's preferences, for example, by using a single interface through which the dedicated input device ports and the general purpose interfaces passes, then enabling or disabling the single interface, as desired, to prevent used input through either the dedicated port or the general purpose port. The system for locking the inputs is subject to various other approaches, including other software, hardware and combination approaches to accomplish the functions desired in a known manner. Thus, many modifications to the system described above can be made without departing from the spirit of the present invention. Accordingly, the foregoing description of the preferred embodiment should be considered as merely illustrative of the principles of the present invention and not in limitation thereof.